Saad Gul
Mike Slipsky

Privacy law:

You need to worry about upcoming European Union regulations

You are a North Carolina company. You have no offices in Europe. Barring the occasional employee vacation, the rare convention or isolated business trip, you have no personnel in the European Union. So do you need to concern yourself with the fact that the European Union's General Data Protection Regulation comes into effect on May 25, 2018? The answer will surprise you. In a word, yes.

By way of background, the GDPR is a European Union regulation. A regulation, as opposed to a directive, automatically becomes binding law throughout Europe on the designated day. Member states are not required to pass their own implementing legislation to render it enforceable. So on May 25, 2018, the GDPR will be the law of the land in all European Union member states. Those member states will include the United Kingdom, since the Brexit withdrawal process will not be complete by May 2018.

The GDPR is built around one fundamental principle: the data subject (the individual) has the right to control his or her data. Contrary to popular belief, the GDPR does not apply to all data. It applies only to personally identifiable information or certain types of personal data that can be connected to an individual resident of the European Union. As the result of Europe's recent historical experience with data collection at the hands of totalitarian regimes, the European Union approaches data processing with far greater wariness than the United States.

In the United States, any data processing that is not specifically prohibited, such as health information by HIPAA or educational records under FERPA, is generally permissible. The European Union takes the opposite approach. Unless a specific exemption is available — typically based on the individual data subject's permission or "the legitimate needs of the data processor — data processing is forbidden.

So why should a North Carolina company care? Frst, the GDPR applies to any entity worldwide that processes an EU resident's personal data. And many companies process more data than they may appreciate. Do you have a website? Do you utilize any sales and prospect tracking software? If either the website or the software handles the personal data of EU residents, that potentially constitutes processing. In other words, many technology and other companies that do not consider themselves to be traditional data processors — those involved in advertising, education or training — may still be subject to the GDPR.

Second, even if a company's business is not built around the collection, processing or handling of personal data, it will inevitably find that routine functions necessitate the incidental processing of personal data. Data processing regulations directly and self-evidently affect companies handling core data processing functions such as payroll or social media analytics. But the GDPR definition of processing is much broader. It encompasses virtually every conceivable category of personal data.

As a result, we have already advised medical supply, manufacturing and transportation companies regarding the new regime. These businesses could not be farther removed from the Silicon Valley behemoths from Central Casting that dominate most commentary on the FDPR. They are not Big Data mammoths such as Google, Facebook or their equivalents. But routine managerial operations in even the oldest and most traditional brick-and-mortar businesses can entail the processing of EU resident data, such as to bill orders to the right individual or to ensure that deliveries are routed to the correct address. That processing carries obligations.

At this point you may find yourself saying: Both those points entail dealing, and perhaps merely tangential dealing, with clients or individuals located in the European Union. None of my clients are located there. Is GDPR still an issue? Once again, the answer is yes.

Our third point is that domestic companies servicing domestic customers will find that those domestic customers oftentimes need to process EU resident data for their own business operations. To retain those domestic customers, the company needs to become GDPR compliant. If it does not, it runs the very real risk of risk losing that customer's business to a competitor who is.

For example, North Carolina has a well established and growing technology sector. Those familiar with the technology industry know that the vendor-client relationship does not entail a single cash-and-carry transaction. The relationship will almost certainly encompass additional services such as installation, training, consulting, customization, servicing, troubleshooting and updates. Indeed, these separate modules typically constitute a significant portion of the revenue booked against a particular relationship.

So if the technology company's own clients service EU residents, then those additional premium services will entail data processing. And should the North Carolina company have a single client that uses its product to handle EU resident data, it must comply with the GDPR. Of course, some activities, such as training, could be undertaken using dummy data. No GDPR compliance would be required in those instances. However, most premium activities, such as upgrades, legacy data migration, cloud implementation or customization, necessitate some level of data processing. And if that data processing involves the personal data of EU residants, they will require GDPR compliance.

Fourth, if the North Carolina company is ever sold or acquired, GDPR compliance will be a factor in the acquisition. We have already seen queries specifically addressing GDPR compliance representations and warranties in due diligence documentation. Many buyers consider GDPR compliance as a non-negotiable prerequisite in an acquisition. Even if it's a negotiable issue for the buyer, the perceived value of the enterprise will be affected by a lack of compliance. So, too, will the terms of the acquisition.

Fifth, the overlap between various privacy regimes means that the GDPR will become the de facto global data processing standard. GDPR provisions require that any processing of any EU resident's data anywhere in the world comply with certain requirements. The practical implication of the GDPR effect of this requirement is that even if a North Carolina company undertakes a joint enterprise with a non-European Union partner, the partner has a business incentive to require GDPR compliance. For example, consider a North Carolina company with a longstanding and profitable relationship with a channel partner in Singapore. Singapore is not part of the European Union. Therefore, the GDPR would appear to have no relevance to the relationship. But it does.

The Singapore partner will have the same concerns that domestic customers do — the loss of business to GDPR-compliant competitors. If the Singapore partner has clients, either resident in the European Union or clients who process EU resident data, then it is faced with two choices: It could forgo a considerable volume of business, or it could become GDPR-compliant. Part of its compliance efforts would entail requiring its partners – the North Carolina company in the hypothetical – to adhere to GDPR requirements. What does this mean for the North Carolina company? It also faces two choices: It could lose the Singapore partner to a GDPR-compliant competitor, or it could become GDPR-compliant itself.

In 1808, Lord Ellenborough protested against worldwide jurisdiction asking, "Can the island of Tobago pass a law to bind the rights of the whole world ? Would the world submit to such an assumed jurisdiction?" Two centuries later, his question appears to have been answered. When it comes to data protection, Brussels can indeed evidently pass a law that binds the rights of the world. North Carolina businesses need not submit to such jurisdiction. But in doing so, they will abandon a significant portion of global business.

Saad Gul and Mike Slipsky, editors of NC Privacy Law Blog, are partners with Poyner Spruill LLP. They advise clients on a wide range of privacy, data ssecurity and cyber liability issues, including risk management plans, regulatory compliance, cloud computingimplications and breach obligations. Saad Gul (@NC_Cyberlaw) may be reached at 919-783-1170 or sgul@poynerspruill.com. Mike Slipsky may be reached at 919-783-2851 or mslipsky@poynerspruill.com.

SAAD GUL focuses his practice on privacy and information security. He advises clients on a wide range of privacy, data security and cyber liability issues, including risk management plans, regulatory compliance, cloud computing implications and breach obligations. In advising his clients on these issues, he often draws on his technical background and prior career as an information-technology consultant. In addition to his privacy practice, Saad also represents clients in complex commercial litigation, regulatory disputes and antitrust matters. He has handled high-profile litigation in state and federal appellate courts across the country, including the U.S. Supreme Court.

MIKE SLIPSKY is an attorney in the business organizations group and has practiced with the firm since 2005. He focuses his practice on mergers and acquisitions for companies across a broad range of industries. He represents buyers and sellers in mergers, acquisitions and divestitures. He also counsels clients on a variety of privacy and information security matters, including HIPAA compliance and data-breach prevention and responses. Additionally, he advises clients on a broad range of corporate and securities matters, including corporate reorganizations and restructurings, commercial contracts, corporate governance, the formation and maintenance of business entities, and securities offerings.